

6. CLAIMS

1. A processing method for performing a symmetric-
key encryption process utilizing an information processing
5 device, comprising the steps of:

(1) performing an encryption process $Z = E(M, K)$
in which a secret key K is to be applied to an input
plaintext M , and for storing a processing result Z in a
memory;

10 (2) performing a decryption process $W = D(Z, K)$
for said process result Z on said memory and storing the
decryption result W on the memory;

(3) outputting said processing result Z when said
processing result W coincides with said plaintext M ; and

15 (4) suppressing the output of said processing
result when said processing result W does not coincide
with said plaintext M .

2. An encryption processing method of claim 1
wherein said encryption process and said decryption
20 process are executed according to the DES (data encryption
standard).

3. An encryption processing method of claim 1
wherein said information processing device is reset as a
control method of suppressing the output of said
25 processing result.

4. An encryption processing method of claim 1 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit to be mounted on an IC card.

- 5 5. A method for performing symmetric key decryption process utilizing an information processing device, comprising the steps of:

(1) performing a decryption process $Z = D(C, K)$

- wherein a secret key K is to be applied to an input
10 ciphertext C, and storing the processing result Z on a memory;

(2) performing an encryption process $W = E(Z, K)$ for the processing result Z on said memory, and storing the result W on the memory;

- 15 (3) outputting said processing result Z when said processing result W coincides with said ciphertext C; and

(4) suppressing the output of said processing result when said processing result W does not coincide with said ciphertext C.

- 20 6. A decryption processing method of claim 5 wherein said encryption process and said decryption process are executed according to the DES (data encryption standard).

7. An encryption processing method of claim 5
25 wherein said information processing device is reset as a

method of suppressing the output of said processing result.

8. An encryption processing method of claim 5 wherein said information processing device and said memory are respectively an arithmetic processing unit and a storage unit to be mounted on an IC card.

9. A method for performing an asymmetric key decryption process utilizing an information processing device, comprising the steps of:

- (1) performing a decryption process $Z = D(C, X, J)$ wherein a secret key X and a public key information J are to be applied to an input ciphertext C and storing the result Z in a memory;

- (2) performing an encryption process $W = E(Z, J)$ for the result Z on said memory and storing said result W on the memory;

(3) outputting the processing result Z when said processing result W coincides with said ciphertext C ; and

- (4) suppressing the output of the processing result when said processing result W does not coincide with the ciphertext C .

10. An encryption processing method of claim 9 wherein said encryption process and said decryption process are executed according to RSA cryptosystem.

11. An encryption processing method of claim 9 wherein said information processing device is reset as a

method of suppressing the output of said processing result.

12. An encryption processing method of claim 9
wherein said information processing device and said memory
apparatus are respectively an arithmetic processing unit
5 and a storage unit to be mounted on an IC card.